Semester Project

CS-627: Cryptology
Fall 2004

For the semester project, you will produce a report on one of the following encryption algorithms (See, for example, http://www.tropsoft.com/aboutenc.htm and http://en.wikipedia.org/wiki/Data_Encryption_Standard):

1. Twofish**: See http://www.schneier.com/twofish.html
2. MARS**
3. Serpent**: See http://www.cl.cam.ac.uk/~rja14/serpent.html
4. Skipjack
5. IDEA
6. NewDES
7. SAFER
8. FEAL
9. RC6**
10. CAST-256
11. CRYPTON
12. DEAL
13. DFC
14. E2; See http://info.isl.ntt.co.jp/e2/
15. FROG; See http://www.tecapro.com/aesfrog.html
16. Hasty Pudding Cipher (HPC): See http://www.cs.arizona.edu/~rcs/hpc/
17. LOK197: See http://www.unsw.adfa.edu.au/~lpb/research/loki97/
18. MAGENTA
19. MARS: See http://www.research.ibm.com/security/mars.html

20. Testing of AES Candidates (Round 1): http://csrc.nist.gov/CryptoToolkit/aes/

** indicates algorithm was considered in the final competition for AES.

Please coordinate with each other, so that everyone takes a different algorithm.

Paper **not to exceed** 10 pages including figures. Presentation **not to exceed** 30 minutes.

Pick and choose what is important or special about your algorithm.